Fábrica de Noobs

Desmistificando: urna eletrônica

Natanael Antonioli

Novembro de 2022

1. SUMÁRIO

2. O QUE É UMA ELEIÇÃO JUSTA?

No vídeo anterior (https://www.youtube.com/watch?v=S-9FdNbuRn4) verificamos, por meio da análise dos resultados, que **não existem evidências estatísticas de que houve fraude nas eleições de 2022** – e que **os argumentos alegando o contrário são infundados**.

É então o momento de discutirmos, em caráter atemporal, a segurança da urna eletrônica brasileira. Nesse vídeo, procuraremos responder à pergunta feita por muitos: a urna eletrônica é segura?

Antes de respondermos a essa pergunta, precisamos entender o que exatamente o termo "segurança" significa, afinal, existem várias facetas para essa palavra. Mais especificamente, existem vários requisitos (https://inscrypt.dcc.ufmg.br/o-mito-da-urna-1-1.pdf) que uma eleição justa precisa satisfazer. Eles são:

A. **Somente eleitores legítimos podem votar**: toda eleição tem um conjunto finito de pessoas que têm o direito de votar, e apenas elas podem votar na eleição.
B. **Um eleitor pode votar no máximo uma vez**: não é permitido que um eleitor vote mais de uma vez.
C. **Depositar o voto é um ato confidencial e, em nenhuma circunstância, nem mesmo com a conivência do eleitor, deve ser possível deduzir qualquer informação sobre a opção escolhida pelo eleitor**: isso garante que o eleitor possa exercer seu direito ao voto sem risco de qualquer repercussão por sua escolha, e impede que o eleitor possa vender seu voto.
D. **O eleitor pode verificar seu voto, se certificando que o voto é válido, e pode rever seu voto antes de se comprometer**: depois de ter criado seu voto, mas antes de depositá-lo, o eleitor deve ter a oportunidade de corrigir ou revisar sua cédula.
E. **O eleitor pode se convencer de que seu voto está incluído no conjunto de votos apurados**: esse requisito é o mais difícil de ser satisfeito, dada a necessidade do sigilo do voto.

F. **Não deve ser possível que alguém remova ou modifique uma cédula, bem como adicione cédulas provenientes de eleitores ilegítimos:** os votos representam a vontade (anônima) dos eleitores, e qualquer modificação alteraria essa vontade.

G. **Todos os votos permanecem secretos até o fim da votação:** não deve ser possível apurar a votação durante seu curso, uma vez que isso violaria o sigilo do voto e pode influenciar o voto de quem vota mais tarde.

H. **Todas as cédulas válidas encontradas na urna, e somente aquelas, serão incluídas na contagem:** votos escritos em uma cédula inapropriada ou votos ambíguos não devem ser contados.

I. **A apuração acontece numa sessão pública e verificável:** partidos políticos e observadores neutros podem acompanhar e verificar o processo.

J. **Deve ser possível auditar a contagem:** deve haver um processo de auditoria que convirja para um resultado que todos concordem.

Através desse vídeo, verificaremos como que a urna eletrônica se propõe a fornecer cada um desses requisitos, se e como ela falha em alguns deles, e como que ela pode ser modificada para resolver esses problemas.

3. QUAIS SÃO OS MODELOS DE URNA ELETRÔNICA E COMO ELA FUNCIONA?

Na eleição de 2022, seis modelos de urna eletrônica foram usados, denominados UE2009, UE2010, UE2011, UE2013, UE2015 e UE2020. Conforme verificado em https://www.justicaeleitoral.jus.br/urna-eletronica/informacoes-tecnicas.html, as urnas diferem em aparência e especificações de componentes como processador, tamanho da memória flash, leitor biométrico e bateria.

Figura 1: modelos de urna 2009 a 2020.

O software das urnas é composto de diversos arquivos, e **a maior parte deles é idêntica para todos os modelos**, conforme você pode checar pelo fato de que os resumos digitais da maioria dos arquivos são idênticos independente do modelo (https://www.tse.jus.br/eleicoes/urna-eletronica/seguranca-da-urna/hash/resumos-digitais-hash-dos-sistemas-eleitorais).

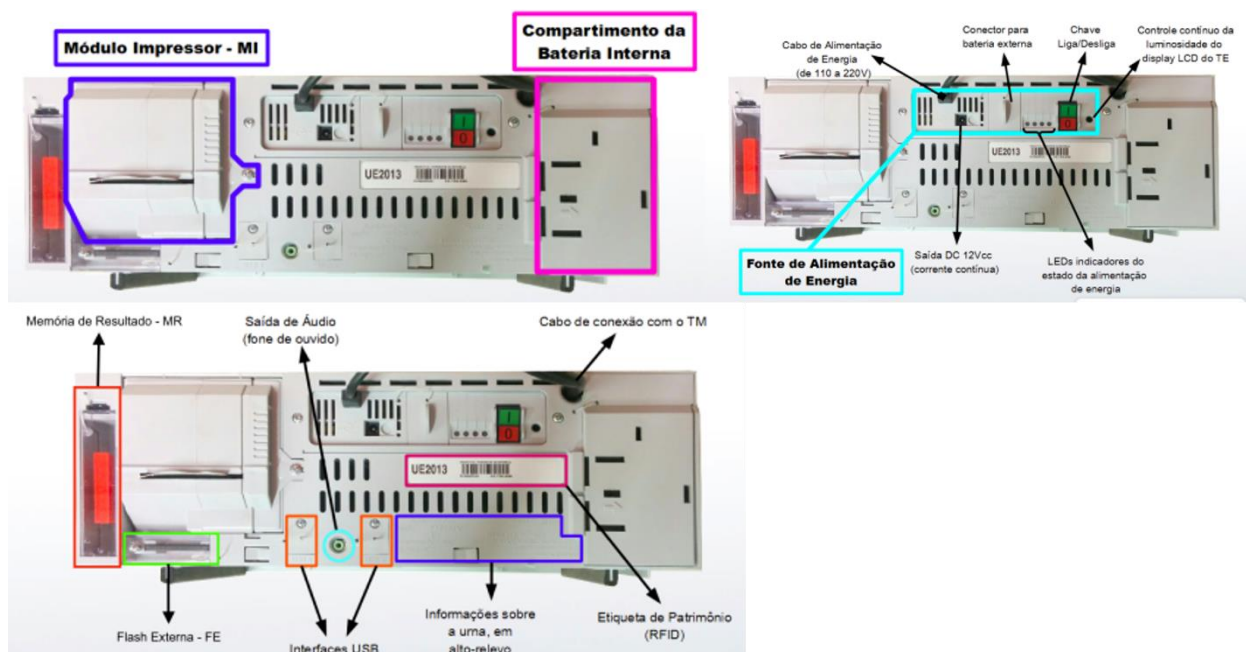
Dentre esses arquivos, uma parte é o núcleo comum presente em toda urna daquele modelo, e outra parte é restrita ao estado da federação (ou cidade no caso de eleição municipal), pois contém dados dos candidatos que disputam aquele turno.

Todas as urnas em utilização são compostas de basicamente dois módulos: um terminal do mesário (TM), onde o presidente da mesa habilita o título de eleitor do eleitor que comparece para votar, e um terminal do eleitor (TE), com o qual o eleitor interage para registrar seu voto.

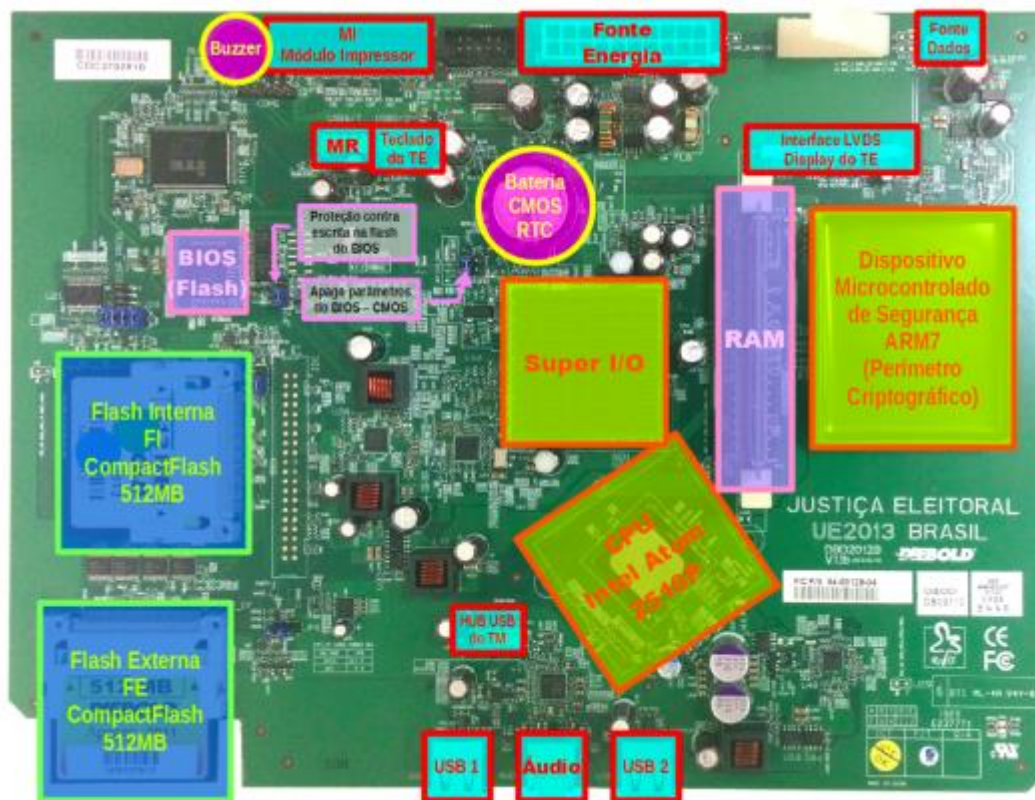
A parte frontal do terminal do eleitor possui uma tela LCD e um teclado numérico com os números na mesma disposição de um telefone, além das teclas Branco, Corrige e Confirma. O teclado possui um circuito resinado (que dificulta acessos não autorizados).

O terminal do mesário também conta com teclado numérico, além das teclas Corrige e Confirma e um display que pode ser alfanumérico (no caso de modelos antigos) ou LCD (no caso do modelo 2020), que exibe informações relevantes como códigos especiais, nome do eleitor, quantidade de eleitores na seção, horário, etc. À direita do teclado numérico, existem 4 leds indicadores de Segurança, Bateria Interna, Aguarde e Liberado, além de um leitor de Smartcard e ma interface USB.

Na parte traseira, temos um módulo impressor (que serve para impressão dos boletins de urna), um compartimento que contém uma bateria interna com autonomia de 12 horas, uma série de conectores de energia para alimentação 110 ou 220 V, bateria externa, chave liga-desliga e ajuste de brilho do display LCD. Há ainda um conector para memória de resultado (MR) e para Flash Externa (FE).

Figura 2: traseira do Terminal do Eleitor.

No interior do dispositivo, temos uma placa mãe, que se conecta com todas as interfaces externas. Além disso, ela possui uma flash interna (FI), um processador, uma memória RAM, um dispositivo microcontrolador de segurança, uma BIOS e uma bateria para a BIOS (garantindo que seus dados nunca se percam).

Temos ainda o dispositivo microcontrolado de segurança (MSE), que é o componente mais importante na segurança da urna eletrônica. Trata-se de um sistema computacional independente (com processador, firmware e RAM próprios), que encontra-se segregado e resinado em um perímetro criptográfico da placa mãe.

Figura 3: placa mãe da urna eletrônica.

As urnas modelo 2009 a 2015 foram produzidas pela Diebold, ao passo que as urnas modelo 2020 foram produzidas pela Positivo. Muitas notícias circulam de que a Smartmatic, empresa do ramo, teria envolvimento na produção de urnas eletrônicas, e que isso seria suspeito porque a empresa possui uma reputação ruim nos Estados Unidos (https://timesofsandiego.com/wp-content/uploads/2022/09/SMARTMATIC-ANSWER-OAN.pdf), seu CEO teria até mesmo sido preso pelo FBI.

Ao passo que houveram discussões sobre a segurança dos sistemas da Smartmatic nos Estados Unidos (tanto que a companhia processou a Fox News por difmação - https://www.smartmatic.com/media/article/faq-defamation-lawsuit-against-fox-corporation/), **é falso que seu CEO, Antonio Mugica, tenha sido preso pelo FBI**. Além disso, a companhia **não fabrica urnas para o TSE e não estava envolvida nas eleições de 2022, tendo apenas prestado serviço de transmissão de dados e voz**.

Existem 5 principais softwares da urna eletrônica: o MSE, o bootloader, a BIOS, e o sistema operacional UENUX. A BIOS (sigla para *Basic Input Output System*) é desenvolvida pela Diebold, e é gravada em memória não volátil, contendo o código necessário para comunicação entre os dispositivos, se mantendo independente da urna possuir ou não fonte de energia.

O *bootloader* é um pequeno código desenvolvido pela SEVIN (Seção de Voto Informatizado do TSE) cuja função principal é carregar o sistema operacional para a memória RAM a partir de duas possíveis fontes: a flash externa ou a flash interna. O sistema operacional UENUX é uma distribuição Linux de uso exclusivo nas urnas eletrônicas brasileiras, também mantido pela SEVIN.

Por fim, o MSE (dispositivo microcontrolado de segurança) possui um firmware desenvolvido pela Diebold, que conta com um hardware para geração de números verdadeiramente aleatórios a serem utilizados na geração de chaves criptográficas, além de realizar a verificação dos demais arquivos da urna.

4. COMO GARANTIMOS QUE O SOFTWARE DA URNA ELETRÔNICA NÃO POSSUI ROTINAS MALICIOSAS?

A Justiça Eleitoral permite (https://www.tse.jus.br/comunicacao/noticias/2016/Maio/desenvolvimento-dos-sistemas-da-urna-podem-ser-acompanhados-por-partidos-e-instituicoes) que diversas instituições, denominadas entidades fiscalizadoras, **tenham acesso ao código fonte dos programas envolvidos no processo eleitoral durante seu desenvolvimento**. São entidades fiscalizadoras (https://www.tse.jus.br/++theme++justica_eleitoral/pdfjs/web/viewer.html?file=https://www.tse.jus.br/comunicacao/noticias/arquivos/respostas-as-forcas-armadas-em-relacao-ao-processo-eleitoral-16-02-2022/@@download/file/TSE-Respostas-%C3%A0s-For%C3%A7as-Armadas-16-02-2022.pdf):

- Partidos políticos, federações e coligações;
- Ordem dos Advogados do Brasil (OAB);
- Ministério Público;
- Congresso Nacional;
- Supremo Tribunal Federal (STF);
- Controladoria-Geral da União (CGU);
- Polícia Federal;
- Sociedade Brasileira de Computação;
- Conselho Federal de Engenharia e Agronomia (CREA);
- Conselho Nacional de Justiça;
- Conselho Nacional do Ministério Público;
- Tribunal de Contas da União (TCU);
- Forças Armadas;
- Confederação Nacional da Indústria;
- Entidades privadas brasileiras sem fins lucrativos com notória atuação na fiscalização da gestão pública;

- Departamentos de tecnologia da informação das universidades credenciadas junto ao TSE.

Isso requer a assinatura de um termo de confidencialidade – portanto, o código fonte permanece fechado – e ocorre em uma sala no TSE, das 13 às 19h, durante um prazo de até 6 meses antes da eleição. Todos os especialistas que adentrem as dependências o fazem portando o mínimo possível de itens, não sendo permitida a

A legislação (https://www.tse.jus.br/legislacao/compilada/res/2015/dje-tse-no-244-de-28-12-2015-p-2-4) determina que a análise poderá ser feita utilizando programas de análise de códigos de conhecimento público e normalmente comercializados. O TSE fornece duas ferramentas: Understanding C e Source Navigator.

A partir da eleição de 2022, iniciou-se um projeto piloto (https://sintse.tse.jus.br/documentos/2022/Fev/17/diario-da-justica-eletronico-tse/portaria-no-107-de-16-de-fevereiro-de-2022-institui-projeto-piloto-com-o-objetivo-de-disponibilizar-) que visa manter o código fonte das urnas eletrônicas em repositórios offline de algumas universidades e entidades, no momento a Polícia Federal, a Universidade Federal de Pernambuco e a Unicamp.

A etapa de desenvolvimento, por afetar diretamente todos os softwares que vão para as urnas eletrônicas, **é considerada por especialistas como a mais crítica em todo o processo**. Atualmente, a única forma de produzir um ataque em grande escala (que afete todas as urnas) **é através de uma conspiração interna no TSE, inserindo código propositalmente falho**, e **a forma de impedir que isso ocorra é através das auditorias realizadas nessa janela de 180 dias**.

Muitos especialistas argumentam que **a abertura pública do código fonte é necessária para que esse elo da cadeia seja devidamente resolvido**. O processo até a abertura total é longo e está longe de terminar, **mas vemos uma tendência gradual em direção à transparência** com, por exemplo, maior número de instituições autorizadas a

auditar o código fonte e projeto piloto para manter o código em computador fora das dependências do TSE.

Antes da introdução do MSE, justificava-se a política de segurança por obscuridade (em que a segurança do sistema dependia de seu funcionamento se mantido em segredo), já que chaves criptográficas privadas podiam ser obtidas através do comprometimento dos flashes de carga. O advento desse módulo fez com que as chaves passassem a ficar confinadas ao perímetro criptográfico na placa mãe, de forma que o comprometimento só é possível com violação da urna e, mesmo que ocorra, compromete apenas a chave daquela urna, pois cada urna tem uma chave distinta.

Dessa forma, há três riscos relacionados a uma falha na auditoria do código fonte, que ocorre durante 180 dias e é liberada para várias instituições: (a) uma rotina propositalmente falha é inserida, suficiente para que o resultado da eleição seja alterado sem nenhuma outra interação, (b) uma vulnerabilidade é propositalmente inserida, que sozinha não causa nada, mas pode ser explorada e (c) uma vulnerabilidade acaba por ficar na urna, que sozinha não causa nada, mas pode ser explorada.

Enquanto o código fonte não for aberto, a competência dessas organizações e a capacidade de auditar o código fonte com as limitações impostas **é o que nos garante que nada do tipo (a) ou (b) ocorreu**. É importante que o TSE fique atento às críticas apontadas por essas organizações, e as corrija de forma a facilitar esse processo de auditoria.

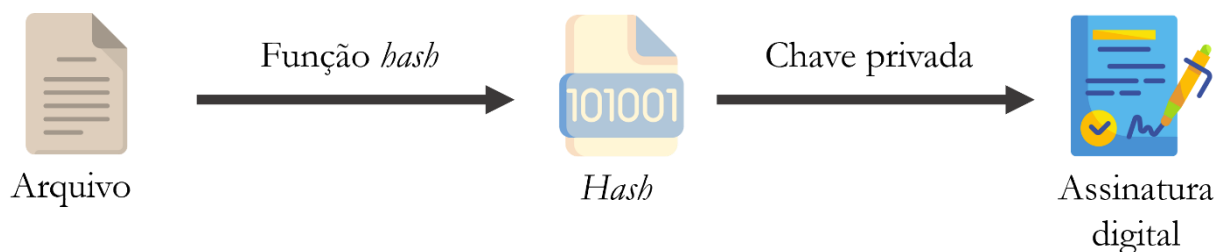
Pessoas contrárias à abertura do código fonte alegam que poderia ficar mais fácil a possibilidade de que uma vulnerabilidade venha a ser descoberta, ignorada e não reportada. É possível que isso ocorra (de forma que um atacante malicioso seja o único a saber de uma vulnerabilidade) mas, conforme veremos a seguir, a cadeia de segurança do processo eleitoral **limita muito o impacto que uma tentativa de fraude possui a partir do momento em que o código fonte é produzido**.

5. Como sabemos que o software auditado não foi modificado?

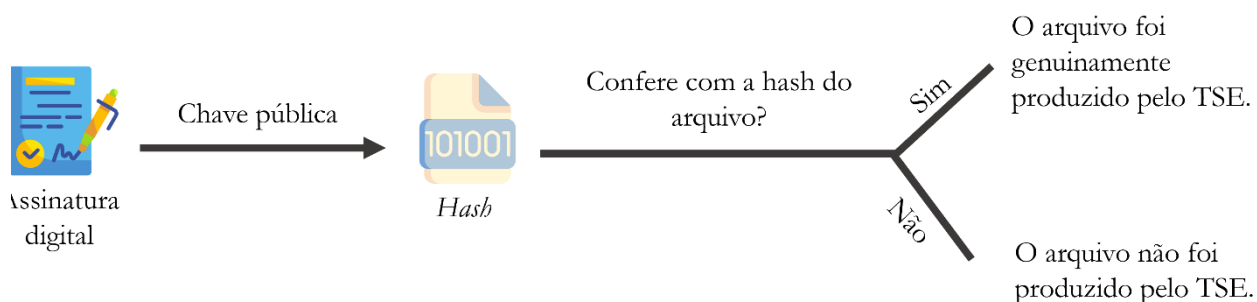
Temos então a Cerimônia de Assinatura Digital e Lacração dos Sistemas (http://www.justicaeleitoral.jus.br/arquivos/tse-resolucao-23-458-instrucao-53-765), que marca o momento em que os programas deixam de ser modificados. Após apresentar os programas para inspeção e validação, eles são assinados digitalmente com chaves privadas que são mantidas em sigilo. Representantes de entidades fiscalizadoras também poderão assiná-los com suas chaves privadas.

Mas o que exatamente é uma assinatura digital? Todos os arquivos envolvidos são passados por uma função resumo (também chamada função *hash*) para obter uma sequência de caracteres derivada do conteúdo do arquivo. Essa sequência é única para aquele conteúdo, e qualquer mínima alteração no conteúdo muda completamente a sequência.

A sequência é então criptografada pelo TSE utilizando uma chave privada que só a instituição tem acesso. O resultado é inserido no arquivo, e temos assim um arquivo assinado digitalmente. Esses arquivos vão para a urna eletrônica e são checados por ela no momento da inicialização, conforme veremos.

Figura 4: os arquivos que vão para a urna eletrônica são assinados digitalmente.

Podemos checar a autenticidade de um arquivo assinado digitalmente em dois passos. Primeiro, calculamos a *hash* desse arquivo. Então, utilizamos uma chave pública (gerada junto com a chave privada) para decifrar a assinatura digital. Se o resultado da decifração for igual à *hash* do arquivo, **então o arquivo foi genuinamente assinado pela entidade que possui aquela chave privada**, pois **é impossível assiná-lo com outra chave privada e produzir**

uma assinatura que, quando decifrada com aquela chave pública, produza o mesmo resultado.

Figura 5: conferência de um arquivo assinado digitalmente.

As entidades que podem auditar o código fonte durante o seu desenvolvimento **também podem assinar digitalmente os arquivos, garantindo que eles não foram modificados depois de serem assinados**. Então, uma página com os resumos digitais de todos os arquivos será produzida e também assinada digitalmente pelo TSE. Essa página pode ser vista em https://www.tse.jus.br/eleicoes/urna-eletronica/seguranca-da-urna/hash/resumos-digitais-hashes-das-eleicoes-2022-1o-e-2o-turnos.

Em seguida, os programas, as assinaturas digitais, a chave pública e os resumos são gravados em mídias não-regraváveis, que são acondicionadas em um invólucro lacrado e armazenadas em um cofre no TSE, **possíveis de serem checados pelas entidades fiscalizadoras a qualquer momento**.

O relatório das Forças Armadas apontou que os computadores do TSE, durante a compilação, acessaram a rede. Esse é um ponto que precisa ver a ser esclarecido, **de forma a entendermos porque esse acesso ocorreu**.

6. COMO O SOFTWARE CHEGA ATÉ AS URNAS?

O software das urnas é transmitido pelo TSE, através de uma VPN, para suas ramificações. Através do o Gerenciador de Dados, Aplicativos e Interface com a Urna Eletrônica (GEDAI-UE), são gravadas às seguintes mídias:

- Flash de carga, com o sistema operacional da urna, todos os seus aplicativos e dados das seções eleitorais selecionadas.
- Flash de votação, com os dados dos candidatos que concorrem na eleição.
- Mídia de resultado, um pen drive especial que armazenará os arquivos com os votos da seção.

O sistema GEDAI-UE possui registro no log com as quantidades e tipos de mídias geradas. A flash de carga serve para entre 50 e 100 seções eleitorais. Cada cartão de memória possui um número serial, que **permite auditar quais seções foram geradas a partir de cada flash de carga**. Um ataque ao flash de carga possui alguma escalabilidade (pois é capaz de afetar múltiplas seções), **mas não é capaz de afetar todas as urnas da eleição**.

A criação dessas mídias ocorre na Cerimônia de Geração das Mídias é anunciada com dois dias de antecedência para ser acompanhada pelas partes interessadas. Então, os cartões de memória são envelopados e guardados até o momento de gravação das urnas.

Isso irá ocorrer na Cerimônia de Carga das Urnas, que é realizada nos Tribunais Regionais Eleitorais ou Cartórios Eleitorais. Partes interessadas também são convidadas a acompanhar a cerimônia, mas especialistas (https://www.researchgate.net/publication/330914587_The_Good_the_Bad_and_the_Ugly_Two_Decades_of_E-Voting_in_Brazil) comentam que **as cerimônias acontecem em tantos lugares que é difícil para os partidos acompanharem todas elas**.

No procedimento de carga, o flash de carga é inserido no espaço da flash externa e a urna é ligada. A urna então verifica todas as assinaturas (por um processo que entenderemos mais adiante) e, se estiver tudo certo, o Software de Carga da Urna Eletrônica (SCUE) solicita

data e hora e o número da seção eleitoral que será carregada na urna. Quando a seção é carregada, ela é marcada no cartão de memória.

O SCUE então formata o cartão de memória presente na flash interna e instala o sistema operacional e todos os aplicativos da urna, além dos eleitores da seção. É então gerado um relatório chamado Extrato de Carga da Urna. Após conferência do relatório, solicita-se que insira a flash de votação no drive da flash externa (para carga dos dados dos candidatos) e a mídia de resultados no slot próprio.

A urna é então ligada, e seu sistema é inicializado a partir da flash interna. A urna então faz um auto-teste que envolve também intervenção do operador, verificando que todos os dispositivos funcionam corretamente. Se tudo funciona bem, uma mensagem de que a urna só funcionará no dia da eleição é exibida, e a urna é desligada e lacrada com lacres confeccionados pela Casa da Moeda, armazenada em uma caixa e devolvida à prateleira onde aguardará o momento de ser distribuída.

Os fiscais de partidos políticos **podem solicitar a auditoria de até 3% das urnas de cada município**. Nessa auditoria, **as assinaturas digitais das urnas e os resumos são conferidos** através de programa disponibilizado pelo TSE, ou através de programas produzidos pelos partidos políticos e homologados pelo TSE na Cerimônia de Lacração. Há, ainda, a possibilidade de simular a votação para checar o funcionamento dos sistemas.

Os seguintes programas são utilizados para fins de fiscalização e auditoria:

- Verificador de integridade e autenticidade de sistemas eleitorais (AVPART), que verifica a equivalência entre os programas instalados nas urnas e os sistemas lacrados.
- Verificador de Assinaturas Digitais (VAD), que averigua a autenticidade dos sistemas eleitorais, utilizando inclusive os programas de verificação das entidades fiscalizadoras assinados digitalmente na Cerimônia de Lacração.
- Verificador de Autenticação de Programas (VAP), que verifica os resumos digitais dos programas.

- Verificador Pré/Pós-Eleição (VPP), que verifica a integridade dos sistemas na urna através da simulação de eleição e da conferência visual dos dados dos candidatos e partidos.

Dessa forma, as entidades fiscalizadoras **podem checar que primeiro que o resumo dos programas na urna é idêntico ao resumo dos programas produzidos na Cerimônia de Lacração**, e **então verificar que eles conferem com os códigos fontes armazenados no cofre**.

Sempre que ocorre a carga da urna eletrônica, é produzido um código de identificação de carga, um identificador único produzido por uma função que associa o código do município, número da seção eleitoral, serial da urna eletrônica, serial da flash de carga, data e hora da carga e um número aleatório, de forma que o código de identificação de carga seja número distinto mesmo que uma nova carga ocorra na mesma urna com os mesmos dados de carga.

Esse código estará presente em vários relatórios emitidos pela urna, como o extrato de carga da urna, a zerésima e o boletim de urna, além de ser um mecanismo de conferência quando o resultado da seção é transmitido ao TSE. A tabela de correspondência das urnas é também publicada na internet (https://dados.gov.br/dataset/resultados-2022-correspondencias-esperadas-e-efetivadas-2-turno).

Para fraudar a urna após a carga, seria necessário inserir um novo cartão de memória ou mídia de resultado, **o que passaria pelo rompimento dos lacres**. Desse momento em diante, um ataque tem pouquíssima escalabilidade, pois afeta apenas uma urna. A única de propaga-lo é realizando-o em todas as urnas.

7. NO DIA DA VOTAÇÃO, COMO A URNA VERIFICA A AUTENTICIDADE DE SEUS ARQUIVOS?

O primeiro componente da urna eletrônica a ser energizado quando esta é ligada é o MSE. Uma das funções do MSE é fazer a leitura e verificar a assinatura da BIOS com a chave pública previamente inserida na urna eletrônica, checando se ela é válida. Entender esse processo é fundamental para compreender como a segurança da urna é garantida.

O MSE, então, recebe cada arquivo (em momentos diferentes dependendo da função do arquivo, conforme veremos) e o decripta utilizando uma chave pública, presente na urna, gerada junto com a chave privada de forma que **a decifração só é possível se o arquivo tiver sido produzido com aquela chave privada**. Se a decifração se der com sucesso e produzir a mesma *hash* que o arquivo possui, então o arquivo foi assinado com a chave privada do TSE – e só o TSE pode fazer isso.

Sendo assim, o primeiro passo é a leitura do software da BIOS pelo MSE e a checagem de suas assinaturas. Se tudo está correto, a BIOS entra em execução. A BIOS é um software desenvolvido pela Diebold, que é gravado em memória não volátil e permanece nela independente da urna ser ou não alimentada com energia.

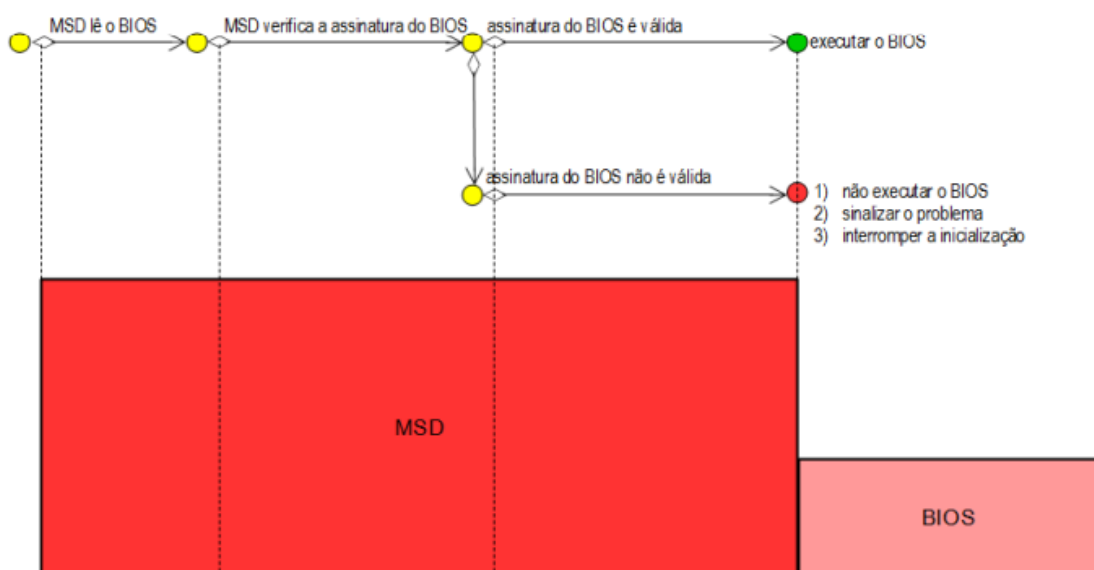
Figura 6: primeiro passo da inicialização.

Então, a BIOS carrega o bootloader (desenvolvido pelo TSE) na memória e verifica sua assinatura através do MSE. O bootloader pode vir da memória flash interna ou da flash externa, por razões que entenderemos mais adiante. Se a assinatura for válida, só então o bootloader entra em execução.

Figura 7: segundo passo da inicialização.

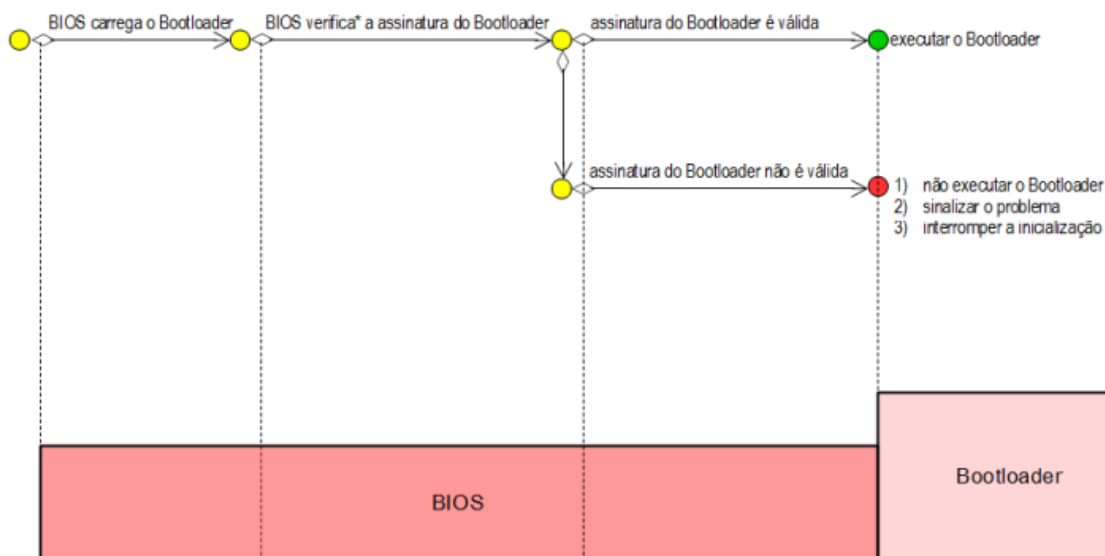
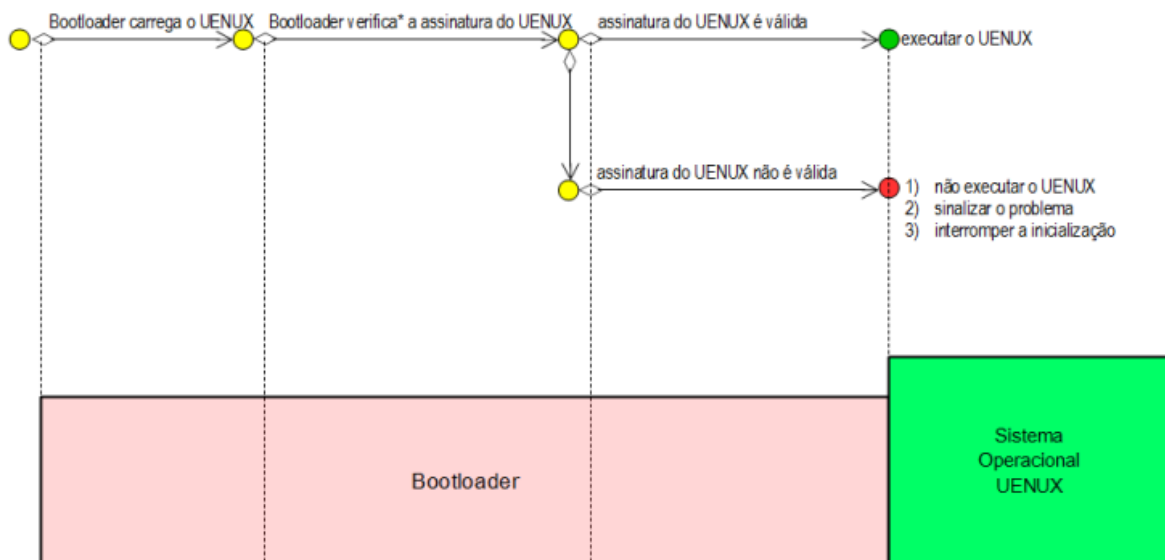
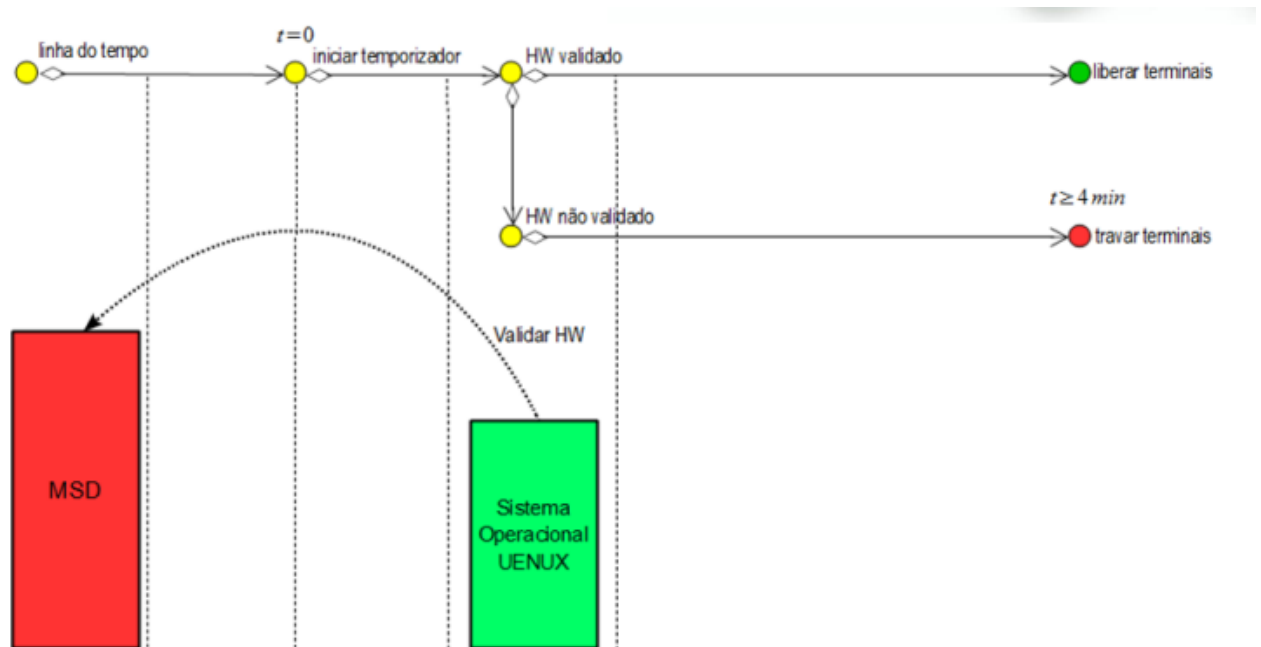
BIOS carrega o Bootloader
BIOS verifica* a assinatura do Bootloader
assinatura do Bootloader é válida
executar o Bootloader
assinatura do Bootloader não é válida
1) não executar o Bootloader
2) sinalizar o problema
3) interromper a inicialização
BIOS
Bootloader

O bootloader decifra o kernel do UENUX, o sistema operacional baseado em Linux desenvolvido pelo TSE, e verifica sua assinatura, colocando-o em execução em seguida.

Figura 8: terceiro passo da inicialização.

Assim que o UENUX entra em execução, ocorre a validação do hardware da urna eletrônica, que é feito através de um protocolo desafio-resposta seguindo os passos abaixo:

1. A aplicação solicita uma chave ao MSE.
2. 1024 bytes aleatórios são gerados com a chave recebida no passo 1.
3. O criptograma é enviado para o MSE.
4. O MSE decifra o criptograma e assina os dados decifrados, enviando-os para a aplicação.
5. A aplicação verifica a assinatura através do MSE.

Figura 9: última etapa da inicialização.

Assim, **toda essa cadeia serve para garantir que todo o código da fonte da urna foi inserido pelo TSE e não por terceiros**, afinal, nenhum terceiro possui a chave privada do TSE para produzir arquivos assinados digitalmente.

8. O QUE ACONTECE NO MOMENTO DA VOTAÇÃO?

Na manhã do dia eleição, a tela da urna exibe a mensagem para emissão da zerésima. A zerésima é um comprovante que indica que não há registros de votos na urna eletrônica, e é obrigatório para a ata da seção. Ele traz, além de informações da seção e da urna (como data e hora da carga e código de identificação de carga), a relação de todos os candidatos aptos com o voto zerado.

O sistema entre em modo de votação às 8 da manhã. O eleitor que checar apresenta um documento com foto ao mesário, que procura seu nome no caderno de votação. Encontrando eleitor, o mesário pronuncia o número do título ao presidente da mesa, que o digita no terminal do mesário.

A urna verifica se o número do título digitado existe no arquivo de eleitores, e exibe no terminal do mesário uma mensagem de confirmação com o nome do eleitor. Na votação sem biometria, o mesário confirma o nome do eleitor e o eleitor se dirige à cabine de votação, dando margem a alguns problemas frutos da desatenção do mesário, nos quais eleitores votam no lugar de outros.

Na votação com biometria, após exibir o nome do eleitor para confirmação, a urna solicita que o eleitor posicione um dedo para identificação biométrica em 4 tentativas, que, caso falhadas, permitem que a votação prossiga a partir da inserção do ano de nascimento do eleitor no terminal do mesário, uma informação que não consta no caderno de votação e que **dificulta a possibilidade de o mesário votar por eleitores faltosos**.

Um vídeo que circulou na internet (https://www.justicaeleitoral.jus.br/fato-ou-boato/checagens/mesaria-manipulou-video-para-dar-a-entender-que-seria-possivel-votar-por-eleitor-faltoso/#0) traz uma mesária mostrando como é fácil votar por eleitores faltosos, mas **suprime a parte de que é preciso informar o ano de nascimento do eleitor**.

O software de votação, então, exibe para o eleitor o cargo para o qual deve ser registrado o voto, em uma das seguintes ordens:

- Vereador e prefeito para eleições municipais;
- Deputado federal, deputado estadual, senador(es), governador e presidente para eleições presidenciais.

Nos cargos proporcionais, ao digitar os dois primeiros números, a urna exibe a legenda do partido escolhido. Digitar um número inválido de uma legenda válida computará o voto para a legenda. O eleitor então confirma seu voto, ou o corrige, de forma que não é possível corrigi-lo após confirma-lo.

Há um intervalo de tempo para que o eleitor possa conferir seu voto, durante o qual a urna não registrará a tecla Confirma. Se um eleitor não respeitar esse intervalo e pressionar a tecla, não haverá efeito, e será necessário pressioná-la novamente ao final do processo. **Isso não é indicador de fraude**.

Durante esse processo, os votos são armazenados em memória volátil. O registro na flash de votação e na flash interna (através de uma estrutura de dados que compreenderemos na próxima seção) só acontece quando o último cargo é confirmado, e a mensagem de "FIM" paralela ao sinal sonoro ocorre. **Essa redundância é importante para permitir a eventual recuperação dos dados**.

O eleitor que esteja fora de seu domínio eleitoral pode justificar o voto. Isso é feito informando-se o título de eleitor no terminal do mesário, o que faz com que, caso o título não exista nos arquivos daquela urna, a justificativa seja registrada na memória do equipamento.

É impossível impedir que um eleitor que já justificou seu voto dirija-se à sua seção e vote, uma vez que a urna não se comunica com a internet ou com qualquer outro sistema que não o terminal do mesário durante a votação. Porém, **isso não é um problema**: se o eleitor pode votar após justificar, seu voto será computado (afinal, é impossível saber qual dos votos na urna é o daquele eleitor), e a justificativa deixa de valer.

Na eleição de 2014, foram encontrados, de 8 milhões de justificativas, 40 mil casos de justificativas seguidas de votação. Parte desses votos pode ser explicada por eleitores que justificaram mas optaram por votar (por exemplo, ao mudar seus planos e viajar durante o dia

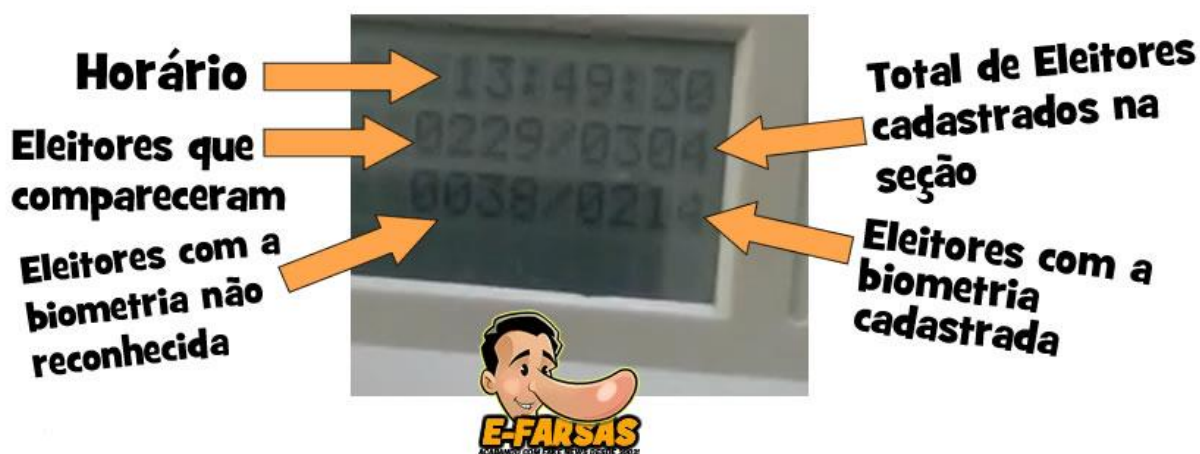
da eleição), mas também porque **o mesário pode ter se enganado na hora de digitar o título do eleitor que procurou justificar e inserido um título válido**. A forma como números de título são gerados torna isso especialmente possível.

Figura 10: exemplo da facilidade em se informar um título de eleitor errado.

006119490426 → Título válido
067119490426 → Luís Fernando Schauren
671194990426 → Título válido

Em outro vídeo (https://www.e-farsas.com/urna-eletronica-deu-voto-para-o-lula-e-para-o-bolsonaro-ao-mesmo-tempo.html) a mesária mostra um registro no terminal do mesário que supostamente indica o total de votos que cada candidato teve e, quando dois números incrementam em 1, afirma que o eleitor votou para ambos os candidatos.

Porém, essa informação é falsa (https://www.e-farsas.com/urna-eletronica-deu-voto-para-o-lula-e-para-o-bolsonaro-ao-mesmo-tempo.html): **o terminal do mesário não mostra o número de votos que cada candidato teve**, mas sim o total de eleitores que compareceram e o total de eleitores com a biometria não reconhecida.

Figura 11: se ambos os números aumentaram, então o eleitor votou e não teve a biometria reconhecida.

É também importante lembrar que os partidos políticos podem nomear fiscais para as seções, **o que limita bastante a possibilidade de fraude por parte dos mesários**, seja ela

tirando proveito das etapas do processo (votando no lugar do eleitor, por exemplo) ou atuando de forma indevida (coagindo eleitores a votar em certo candidato, por exemplo).

Mesários podem cometer erros, e esses erros humanos **podem ser desde inofensivos até afetar votos individuais**. Por exemplo, um mesário no 1º turno (https://www.justicaeleitoral.jus.br/fato-ou-boato/checagens/comprovante-de-votacao-do-segundo-turno-foi-entregue-por-engano-a-eleitor-do-para) entregou dois comprovantes de votação (ao invés de só 1) por engano, **mas isso não impediu o eleitor de votar no segundo turno**.

Outros casos são mais graves (https://www.justicaeleitoral.jus.br/fato-ou-boato/checagens/erros-humanos-causaram-confusoes-que-geraram-boatos-no-1o-turno-de-2022/). Se o mesário tentar inserir o título de eleitor de alguém que já votou, um erro aparecerá **– e algumas pessoas foram confrontadas com esse erro mesmo sem ter votado**.

Isso acontece porque, em momento anterior, o mesário digitou o título do eleitor errado e a urna foi liberada. Se a pessoa que votou no lugar puder ser identificada, então a situação pode ser revertida, **mas se isso não for possível o eleitor prejudicado não pode votar**, recebe uma declaração de comparecimento sem voto e é aconselhado a registrar o problema em uma delegacia.

Por fim, muitos especialistas apontam que o fato da urna armazenar os títulos de eleitores aptos a votar naquela seção **pode permitir que haja quebra do sigilo do voto por um atacante que intercepte as comunicações entre os componentes da urna**, apesar de não haver evidências de que isso tenha ocorrido em algum momento.

9. O QUE OCORRE SE UMA URNA APRESENTA DEFEITO?

Urnas podem apresentar defeito, **e é perfeitamente normal que uma pequena fração delas apresente**. Em 2018, por exemplo, uma urna não registrava votos para presidente (https://www.justicaeleitoral.jus.br/fato-ou-boato/checagens/urna-que-nao-permitia-votacao-presidente-apresentou-defeito-e-foi-substituida/#).

O primeiro passo caso uma urna apresente defeito é registrar a ocorrência na ata da seção. Constatado o problema e a impossibilidade de solucioná-lo, uma nova urna – sem mídia de resultados ou flash de votação – é trazida para seção.

A mídia de resultados e a flash de votação da urna defeituosa são inseridas na urna de contingência, que é lacrada com lacres de reposição assinados pelos integrantes da mesa. A urna defeituosa também é novamente lacrada pelo mesmo procedimento.

Pode ser que o problema não esteja na urna, mas na flash de votação. Nesse caso, uma flash de contingência sem dados de eleitores ou de votação é inserida na urna e os dados presentes na flash interna são copiados para a flash de contingência, que passa a ser utilizada.

Caso isso não funcione, a votação é feita em cédulas de papel que são depositadas em uma urna de lona previamente lacrada. Todos os procedimentos de contingência realizados também devem constar na ata da seção.

Um problema da urna pode ser percebido pelo eleitor, que reporta o ocorrido para o mesário. Porém, em muitos casos, **o problema não está na urna, mas nas ações do próprio eleitor**. Em um caso de Vargeão (https://www.justicaeleitoral.jus.br/fato-ou-boato/checagens/e-falsa-alegacao-de-que-urna-eletronica-de-vargeao-sc-exibia-fotografia-de-outra-candidatura-ao-cargo-de-presidente/#), o eleitor afirmou que a foto do candidato era diferente da sua escolha, mas, ao ser orientado a pressionar a tecla Corrige, o problema se solucionou – **indicando que ele provavelmente apenas digitou o número errado**.

Uma eleitora de Curitiba (https://www.justicaeleitoral.jus.br/fato-ou-boato/checagens/e-falso-que-eleitora-nao-teve-voto-computado-em-curitiba-pr/#) alegou não ter conseguido votar para presidente e teve sua reclamação registrada na ata, mas nenhum outro eleitor experimentou o mesmo problema, **indicando possível confusão.**

Outros eleitores agem de má fé para apontar erros que não aconteceram, como um eleitor de Bauru (https://www.justicaeleitoral.jus.br/fato-ou-boato/checagens/eleitora-de-bauru-sp-distorceu-informacoes-sobre-biometria-e-confundiu-numero-de-candidatura-para-cargo-de-deputado/#) que alegou que eleitores eram obrigados a fazer o cadastro biométrico no momento da votação. Isso não acontece, pois **não é feito cadastramento no momento da votação**.

Já um eleitor, para simular um problema na urna, **pressionou duas teclas simultaneamente, fazendo com que o equipamento não registrasse nenhum comando** (https://www.justicaeleitoral.jus.br/fato-ou-boato/checagens/eleitor-pressionou-duas-teclas-ao-mesmo-tempo-para-simular-problema-na-votacao-para-presidente-em-novo-hamburgo-rs/#).

10. COMO VOTOS SÃO COMPUTADOS E TRANSMITIDOS?

Cada voto inserido na urna eletrônica é registrado individualmente de forma digital através de uma estrutura chamada Registro Digital do Voto (RDV). Trata-se de uma tabela do tamanho do total de eleitores na seção, que é preenchida sorteando-se uma posição para cada escolha. Assim, **é possível contar de forma eletrônica o total de votos que cada candidato teve**, mas **é impossível saber o conjunto dos candidatos que um eleitor anônimo votou, bem como saber qual voto foi computado em qual hora**.

Figura 12: preenchimento do RDV.

Eleitor	Votou?
Eleitor 1	✓
Eleitor 2	
Eleitor 3	
Eleitor 4	✓
Eleitor 5	✓

Vereador	Tipo	Prefeito	Tipo
<Branco>	Branco	92	Nominal
90123	Nominal	91	Nominal
92	Legenda		
		99	Nulo

Um artigo de 2022 (https://jus.com.br/artigos/99287/a-possivel-fraude-eleitoral-do-rdv) alegou que o sigilo do voto poderia ser quebrado utilizando o RDV, uma vez que votos poderiam ser comprados (ou coagidos) fornecendo-se uma instrução para cada eleitor votar (por exemplo, anulando votando em a para governador e b para presidente, sendo a e b números fora do pleito), que então poderia ser pesquisada no RDV. Porém, **esse raciocínio ignora que os cargos são embaralhados no RDV** e que, portanto, essa pesquisa seria impossível. O RDV é tão incapaz de quebrar o sigilo do voto quanto um boletim de urna.

Como **ainda podem haver eleitores aguardando para votar mesmo após as 17 horas**, a votação só termina quando o mesário informa um código no seu terminal. Nesse momento, o sistema automaticamente imprime a 1ª via do Boletim de Urna (BU), que contém a lista de todos os candidatos e legendas que receberam ao menos um voto na urna, além do total de votos nulos e brancos, então a mídia de resultado é gravada, e são impressas obrigatoriamente mais 4 vias, e opcionalmente até mais 15 vias do BU. Uma via do BU deve

ser afixada para porta da seção, mas o relatório das Forças Armadas em 2022 apontou que **muitas seções não o fizeram por erro humano**.

Figura 13: cabeçalho do boletim de urna.

38 colunas com fonte em tamanho normal

1a. VIA → Identificação da cópia do boletim, fonte em tamanho expandido (todas as cópias possuem o mesmo conteúdo abaixo)

Justiça Eleitoral
Tribunal Regional Eleitoral [EE] → Sigla da UF

Boletim de Urna → Título pelo Software de Votação

Eleições Municipais 2016 → Nome do processo eleitoral
1° turno → Nome do pleito
(02/10/2016) → Data do pleito

Eleições 2016 - 1° turno
Consulta 2016 - 1° turno → Nomes das eleições

Município 01392 → Número do município
Município TESTE AB → Nome do município

Zona Eleitoral 0009
Local de Votação 0004 → Exclusivo do Software de Votação e do Recuperador de Dados
Seção Eleitoral 0031

Eleitores aptos 0040
Comparecimento 0010
Eleitores faltosos 0030
Habilitados por ano de nascimento 0004
→ Exclusivos do Software de Votação e do Recuperador de Dados

Código identificação UE 01760649 → Número de série da urna
Data de abertura da UE 02/10/2016
Horário de abertura 17:34:49
Data de fechamento da UE 02/10/2016
Horário de fechamento 18:01:33
→ Exclusivos do Software de Votação e do Recuperador de Dados

RESUMO DA CORRESPONDÊNCIA
336.660 → Seis últimos dígitos do código da carga (fonte em tamanho expandido)

Código Verificador: 0.248.546.277 → Código verificador para impedir erros de digitação no Sistema de Apuração

====================================
Eleições 2016 - 1° turno → Nome da eleição
====================================

====================================

---------------VEREADOR--------------- → Nome do cargo
Partido: 91 - PEsp → Número e sigla do partido; marca o início dos votos para o partido e seus candidatos (somente para cargos proporcionais)
Nome do candidato Num cand Votos
Vôlei 91001 0001
Natação 91004 0001
Votos de legenda 0000
Total do partido 0002

Código Verificador: 1.636.361.627 → Código verificador para impedir erros de digitação no Sistema de Apuração

Figura 14: resto de um boletim de urna.

A mídia de resultado é assinada digitalmente e contém mecanismos de segurança que a impedem de ser modificada, e deverá então ser encaminhada a um cartório eleitoral que contém programas para leitura e transmissão dos dados ao TSE.

Figura 15: mídia de resultado e flash externa.

Os dados são então transmitidos pelo protocolo HTTPs para o TSE, que mais uma vez faz a conferência por meio das assinaturas digitais e então totaliza os votos. O processo de totalização e transmissão **é tido por especialistas como um dos mais transparentes**, uma vez que se pode conferir os dados transmitidos com o valor que consta no BU.

Todos os esforços de auditoria que abordaram a comparação do BU com os resultados apresentados pelo TSE **mostraram concordância de resultados**, bem como iniciativas cidadãs como o Você Fiscal (https://www.vocefiscal.org/).

Há uma cerimônia, denominada Cerimônia de Verificação dos Sistemas Eleitorais (https://www.tse.jus.br/comunicacao/noticias/2022/Outubro/tse-realiza-cerimonia-de-verificacao-dos-sistemas-eleitorais-de-2022), na qual os programas utilizados na totalização são verificados e assinados digitalmente, além de ser impresso um relatório zerésima que atesta a inexistência de votos previamente computados no sistema. Foi nessa cerimônia que as Forças Armadas reportaram o uso de um telão para verificação dos arquivos e sugeriram terminais individuais, **não na auditoria do código fonte**.

11. O QUE É A VOTAÇÃO PARALELA?

Às 9 horas da manhã do sábado de véspera da eleição – quando a maior parte das urnas já foi instalada – ocorre uma cerimônia pública que sorteia de 3 a 5 seções eleitorais por estado, sendo uma obrigatoriamente da capital. Para cada urna sorteada, seu respectivo cartório eleitoral é informado e deverá recolhê-la do local de votação, substituindo-a por outra.

Com base na lista de candidatos da urna, entidades fiscalizadoras e partidos políticos podem preencher cédulas de papel com números dos candidatos, votos brancos e nulos. Essas cédulas, após o preenchimento, são guardadas em urnas de lona – uma para cada urna real.

No dia da eleição, as urnas são ligadas e passam pelos mesmos procedimentos que passariam se estivessem em uma sala real de votação. A zerésima é impressa, e confere-se a seção, data e hora e o código de identificação da carga – **garantindo que a urna não foi modificada para a auditoria**.

A partir das 8 horas, os títulos dos eleitores aptos a votar em cada urna começam a ser sorteados juntamente com uma cédula da urna de lona. A cédula é numerada sequencialmente, seu conteúdo é lido em voz alta e mostrando para uma câmera, e seu conteúdo é então digitado na urna, que é constante filmada – dessa forma, podemos identificar se votos foram erroneamente digitados.

Após as 17 horas pode-se encerrar a votação, com possibilidade de inserir mais votos para simular uma fila de eleitores. No encerramento, **os BUs emitidos pelas urnas são comparados com os resultados das planilhas dos auditores**. Até hoje, **não foi encontrado nenhum caso de divergência**.

Especialistas, porém, apontam que **votações paralelas são mais lentas e não usam biometria, de forma que um software malicioso poderia identifica-las por esse comportamento**, além de que **o pequeno espaço amostral dificulta tirar conclusões sobre todas as urnas do país**.

12. O QUE AS AUDITORIAS CONCLUÍRAM ATÉ O MOMENTO?

Auditar o software antes da eleição é um passo importante, mas especialistas (https://urnaeletronica.info/2018/carta-aberta-de-resposta-a-participacao-do-tse-no-nerdcast-626/ e https://www.researchgate.net/publication/330914587_The_Good_the_Bad_and_the_Ugly_Two_Decades_of_E-Voting_in_Brazil) **apresentam algumas falhas nesse processo**.

O primeiro deles **é o imenso tamanho do código fonte**, que possui cerca de 24 milhões de linhas código ao todo **que precisam ser inspecionadas em sua totalidade**, pois todos os componentes foram desenvolvidos ou ao menos modificados para as urnas eletrônicas. Além disso, o termo de confidencialidade impede que pesquisadores honestos comentem sobre as falhas que encontraram, **ao mesmo tempo que pesquisadores maliciosos podem vazar, em segredo, essas vulnerabilidades para atacantes externos**.

A auditoria de código fonte **é útil para reduzir a possibilidade de que uma rotina maliciosa tenha sido inserida de propósito no sistema**, afinal, algo do tipo deveria passar desapercebido por todos os auditores ou fazer parte de uma conspiração entre todos eles. **Nenhuma auditoria, até o momento, revelou esse tipo de rotina maliciosa**, porém, **muitas revelaram dificuldades em analisar adequadamente o sistema**.

Começamos com a auditoria do PSDB, realizada em 2014, após a derrota de Aécio Neves (http://www.brunazo.eng.br/voto-e/arquivos/RelatorioAuditoriaEleicao2014-PSDB.pdf). No documento, concluiu-se que o sistema não fora produzido visando ser auditado, e por isso continha uma série de obstáculos para esse projeto.

Por exemplo, foi negado acesso ao firmware da BIOS e do MSE, sob a premissa de que isso era parte do hardware e não havia sido incluído na petição inicial. Além disso, a possibilidade de recompilar o código fonte foi negada, bem como o documento de requisitos do sistema (atualmente, esse documento já é público - https://www.tse.jus.br/transparencia-e-prestacao-de-contas/licitacoes-e-contratos/compras/audiencia-publica/coleta-de-sugestoes-para-especificacoes-da-urna-eletronica).

O PSDB não conseguiu acessar diretamente o conteúdo das mídias de votação (sendo isso possível apenas com a ajuda de programas), algo que foi classificado como uma falha grave na auditoria. Também não foi permitido acesso aos compiladores utilizados na produção do executável que vai embarcado nas urnas.

A análise da totalização não encontrou sinais de eventuais fraudes, mas salientou que não havia arquivo que indicasse a evolução da totalização, algo que existiu nessa eleição (https://dadosabertos.tse.jus.br/dataset/resultados-2022).

Hoje em dia, os próprios envolvidos com a auditoria de 2014 (https://www1.folha.uol.com.br/poder/2021/08/antes-critico-feroz-da-urna-eletronica-psdb-agora-diz-que-modelo-ficou-seguro-apos-pressao-do-partido.shtml) **afirmam que o processo se tornou mais transparente em resposta às questões levantadas**.

Em 2018, uma auditoria feita em urnas da Região Sul (https://www.tse.jus.br/comunicacao/noticias/2018/Outubro/auditorias-em-urnas-no-pr-rs-e-sc-reafirmam-confiabilidade-do-voto-eletronico) verificou a integridades das mídias e dos lacres, constatando que os defeitos relatados por eleitores não eram decorrência de fraudes. Um perito do PSL a classificou como frágil por não ter conhecimento do que ocorria dentro da urna, e recebeu acesso ao código fonte (https://www1.folha.uol.com.br/poder/2018/10/para-perito-do-psl-auditoria-de-urnas-eletronicas-foi-fragil.shtml).

Em 2022, o PL encaminhou um relatório para o TSE que alegava vulnerabilidades no processo eleitoral a partir de um relatório de autoavaliação, no qual os próprios funcionários concederam nota zero a alguns critérios (https://static.poder360.com.br/2022/09/PL-Resultados-da-Auditoria-de-Conformidade-do-PL-no-TSE.pdf). Porém, o TSE respondeu que tal relatório sequer era sobre o sistema informatizado das urnas eletrônicas, **mas ao TSE e (seu sistema informatizado em um dos tópicos) como um todo**. O mesmo questionário foi aplicado, também, à instituições como o IBAMA e o INCRA (https://valorinveste.globo.com/mercados/brasil-e-politica/noticia/2022/09/30/relatorio-do-pl-sobre-urnas-evidencia-mentira-ou-ma-fe-no-uso-de-dados-afirma-tcu.ghtml).

Também em 2022 (em documento publicado no dia 15 de novembro – https://cdn.oantagonista.com/uploads/2022/11/PL-Relatorio-Tecnico-Logs-Invalidos-das-Urnas-Eletronicas-v0.7-15-11-2022.pdf) o PL constatou que **os logs de urna modelo 2020 eram os únicos que apresentavam o código da urna em cada linha**. Isso é sem dúvidas um comportamento inesperado, mas **não é critério suficiente para justificar o anulamento da eleição**, especialmente **quando o código de identificação da carga da urna ainda pode ser encontrado no log** independente do modelo. Vale lembrar que essa anomalia ocorreu em ambos os turnos. Outras anomalias apresentadas no relatório, como diferenças na proporção de votos conforme modelo de urna, foram abordadas no vídeo anterior.

A partir do projeto piloto iniciado em 2022, a UNICAMP produziu um relatório após inspeção do código fonte da urna (https://www.tse.jus.br/++theme++justica_eleitoral/pdfjs/web/viewer.html?file=https://www.tse.jus.br/comunicacao/arquivos/relatorio-unicamp/@@download/file/Unicamp%20-%20Relato%CC%81rio%20Final.pdf).

A pesquisa verificou se poderia haver alguma rotina que fosse desencadeada somente no momento da votação real e não durante a votação paralela, mas **nenhum código com esse propósito ou possível de ser explorado com esse propósito foi encontrado**. Também se investigou se se a ordem de inserção dos resultados do RDV poderia comprometer o sigilo de voto, e **não foram encontradas evidências disso**.

Não foram encontrados, no código fonte da urna, casos de mau uso de funções criptográficas, mas se deixou a sugestão de que a função SHA-512, apesar de ainda não ser obsoleta, seja substituída por outra. Por fim, os códigos do aplicativo VOTA (do controle da urna) foram analisados e **nada suspeito foi encontrado**. A única impossibilidade de auditoria foi em relação a um algoritmo denominado GUARANA, utilizado para geração de chave simétrica, que o TSE informou ser confidencial.

Também parte desse projeto piloto foi a UFPE, que produziu seu relatório (https://www.tse.jus.br/++theme++justica_eleitoral/pdfjs/web/viewer.html?file=https://www.tse.jus.br/comunicacao/arquivos/relatorio-

ufpe/@@download/file/Relatorio_Piloto_UFPE_TSE_CodigoFonte.pdf) analisando as instâncias de chamadas para o Google Test e procurando por *test smells* (https://testsmells.org/pages/testsmells.html), más práticas adotadas por desenvolvedores na produção de casos de teste. Algumas instâncias foram encontradas, **sinalizando necessidade de melhor planejamento e padronização nos testes**. O relatório em questão **deu ênfase ao fato de o acesso concedido ter sido, pela primeira vez, irrestrito**.

Em 2022, as Forças Armadas produziram um relatório (https://archive.org/details/oficio-do-ministro-da-defesa-e-relatorio-das-forcas-armadas-1) a partir que procurou auditar o código fonte das urnas. Como com todas as demais instituições, a análise de código fonte se deu em uma sala do TSE, utilizando computadores e ferramentas fornecidas pelo TSE além de possibilidade de utilizar outros softwares do mercado, e portando apenas papel e caneta. Isso, por si só, **não é um problema**: não deve ser necessário trazer dispositivos próprios para a auditoria (isso inclusive implicaria em risco de o código auditado vazar), nem qualquer outro tipo de item. Alguns afirmaram que essa análise se deu em um telão, mas **essa informação é falsa, já que o telão é mencionado apenas na etapa de verificação dos programas de cômputo**.

Porém, outros pontos são razoáveis: apontou-se que **foi possível apenas a análise estática** (em oposição à análise do código durante sua compilação), **não foi permitido o acesso à biblioteca de terceiros** e **não foi possível acessar o controle de versão**, restrições essas que tornaram o processo difícil.

Muitos entenderam o termo “biblioteca de terceiros” como uma comprovação de que a urna se comunica com sistemas de terceiros. Isso é falso, pois a urna, durante a votação, **é lacrada e não tem comunicação com a internet**, e fora dela, **há mecanismos de segurança para garantir que a comunicação ocorra apenas com mídias do TSE**. Bibliotecas de terceiros são trechos códigos desenvolvidos por outras organizações que não o TSE, e que foram incluídos no código fonte da urna eletrônica como ferramentas auxiliares. **Isso é uma característica de qualquer sistema**.

Em https://www.tse.jus.br/++theme++justica_eleitoral/pdfjs/web/viewer.html?file=https://www.tse.jus.br/comunicacao/noticias/arquivos/respostas-as-forcas-armadas-em-relacao-ao-processo-eleitoral-16-02-2022/@@download/file/TSE-Respostas-%C3%A0s-For%C3%A7as-Armadas-16-02-2022.pdf, temos a lista das bibliotecas de terceiros utilizadas no sistema da urna eletrônica.

Há quem argumente que de nada isso vale se as auditorias têm limitações, e que a auditoria do exército é equiparável a "encontrar a arma do crime, encontrar pólvora nas mãos do suspeito, mas não encontrar as digitais do suspeito na arma". Porém **essa é uma analogia forçada e sem equiparação no mundo real**.

Uma melhor analogia seria: você me viu entrar com caixas em minha casa, e suspeitou que eu estivesse movimentando drogas (bolsonaristas viram anormalidades nos dados públicos), mas uma análise do meu histórico de compras mostrou que eu comprei produtos legítimos pela internet (todas as explicações que forneci em https://www.youtube.com/watch?v=S-9FdNbuRn4&t=654s).

Ainda assim, você foi autorizado a vasculhar minha casa em busca de drogas (inspecionar o código fonte) utilizando cães farejadores (ferramentas de inspeção de código fonte do mercado), mas não foi autorizado a tirar fotos do processo (portando apenas papel e caneta). Você não encontrou nada (resultado negativo do relatório), mas a porta de um banheiro estava emperrada e eu não me dispus a consertá-la (bibliotecas de terceiros), você não pode me acompanhar em meus afazeres domésticos (limitação da análise estática) e também não pode saber como a minha casa estava ontem (controle de versão).

Dessa forma, você conclui que não encontrou drogas em minha casa, mas que não pode eliminar completamente essa possibilidade. Da mesma forma, o relatório das forças armadas **não encontrou rotinas maliciosas onde procurou, mas não foi capaz de procurar em tudo**. Isso nos diz que não parece haver rotinas maliciosas onde foi procurado, mas **nada diz sobre onde não procurado**. Em última instância, o relatório esclareceu alguns pontos e manteve a dúvida sobre outros.

13. Quais os resultados dos Testes Públicos de Segurança?

A mera leitura e análise do código fonte **não é suficiente para eliminar a existência de vulnerabilidades**. Foi então desenvolvido o conceito de Teste Público de Segurança (TPS), eventos periódicos em que qualquer brasileiro (https://www.tse.jus.br/o-tse/faq/teste-publico-de-seguranca-tps) pode apresentar um plano de ataque contra os sistemas eleitorais para ser testado e, se confirmado, **ter as vulnerabilidades que o permitiram corrigidas**, para então **convidar os atacantes a realizarem seus ataques novamente e checarem se os problemas foram solucionados**.

A seguir, abordaremos quais ataques bem sucedidos foram realizados em cada teste, deixando de lado aqueles que falharam em revelar quaisquer vulnerabilidades. **Todas as vulnerabilidades identificadas foram corrigidas após serem identificadas**, e **não há evidências de que elas foram exploradas em eleições anteriores**.

Os resultados do teste de 2009 podem ser vistos em https://www.justicaeleitoral.jus.br/++theme++justica_eleitoral/pdfjs/web/viewer.html?file=https://www.justicaeleitoral.jus.br/arquivos/tse-relatorio-final-da-comissao-avaliadora-1o-teste-de-seguranca/@@download/file/TSE-relatorio-final-da-comissao-avaliadora-1-testes-de-seguranca.pdf. Os seguintes ataques tiveram sucesso:

- Foi possível a interceptação de radiação eletromagnética que emanava do teclado da urna, de forma a quebrar o sigilo do voto.
- Foram encontradas algumas fragilidades no processo formal das eleições, como falta de documentação de como as chaves deverão ser guardadas pelo TSE, a baixa amostra de urnas auditadas, a falta de padronização de alguns procedimentos e a pouca significância estatística da votação paralela.
- Foi possível alterar o núcleo do sistema operacional da urna, mas não foi possível validar esse núcleo.

Os resultados do teste de 2012 podem ser vistos em https://www.justicaeleitoral.jus.br/++theme++justica_eleitoral/pdfjs/web/viewer.html?file=https://www.justicaeleitoral.jus.br/arquivos/tse-avaliacoes-sobre-o-teste-de-seguranca-da-urna-eletronica/@@download/file/tse-avaliacoes-sobre-teste-seguranca-urna-eletronica-relatorio-final.pdf:

- Foi possível sequenciar os votos armazenados no RDV, motivando melhorias na forma como eles eram embaralhados.

Os resultados do teste de 2016 podem ser vistos em https://www.justicaeleitoral.jus.br/++theme++justica_eleitoral/pdfjs/web/viewer.html?file=https://www.justicaeleitoral.jus.br/arquivos/tse-testes-publicos-de-seguranca-2016-compendio/@@download/file/TSE-teste-publico-de-seguranca-2016-compendio.pdf:

- O sistema de apuração validou boletins de urna falsos porque não possuía mecanismos de autenticação com assinatura digital.
- Através da saída de fone de ouvido da urna, foi possível violar o sigilo do voto por meio da transmissão de áudio.
- Com violação do lacre da urna eletrônica e contando com uma conspiração de mesários e de fiscais, foi possível utilizar uma urna eletrônica falsa para votação do eleitor, paralelamente à votação feita por um atacante na urna verdadeira com os títulos dos comparecidos.
- Com violação do lacre da urna eletrônica e contando com uma conspiração de mesários e de fiscais, foi possível quebrar o sigilo do voto comparando a memória interna antes e depois de cada eleitor.

Os resultados do teste de 2017 podem ser vistos em https://www.justicaeleitoral.jus.br/++theme++justica_eleitoral/pdfjs/web/viewer.html?file=https://www.justicaeleitoral.jus.br/arquivos/relatorio-tecnico-tps-2017-1527192798117/@@download/file/TSE-relatorio-TPS-2017-teste-confirmacao.pdf:

- Foi possível recuperar uma chave criptográfica embarcada no núcleo do sistema operacional através de engenharia reversa.
- Foi identificado um bug que, através de um valor com sinal sendo salvo em uma variável sem sinal, permitia a execução de bibliotecas adulteradas.
- Foram encontradas duas bibliotecas executadas sem assinatura.
- Modificando uma dessas bibliotecas sem assinatura, foi possível utilizar um teclado externo na urna eletrônica.
- Foi possível iniciar o núcleo do sistema operacional em uma máquina virtual, mas a execução cessou antes de inicializar qualquer aplicativo.
- Verificou-se que, através de um parâmetro de segurança no compilador GCC, um dos ataques poderia ser dificultado.
- Arquivos JPEG tinham um campo de comentário que não era validado. Apesar de não haverem vulnerabilidades associadas a esses arquivos, essa falta de validação poderia vir a ser explorada.

Os resultados do teste de 2019 podem ser encontrados em https://www.justicaeleitoral.jus.br/tps/arquivos/tps_2019_relatorio_final-atualizado_17_12_2019.pdf e https://www.justicaeleitoral.jus.br/tps/arquivos/tps_2019_relatorio_tecnico_atualizado_17_12_2019.pdf:

- O GEDAI-UE (Gerenciador de Dados, Aplicativos e Interface com a Urna Eletrônica), quando executado em ambiente Windows, é criptografado por um sistema chamado SIS. Foi possível, possuindo senhas de acesso à BIOS, obter a chave utilizada na criptografia, possibilitando acesso aos programas do GEDAI-UE.
- Através do GEDAI-UE, foi possível gerar uma mídia de carga maliciosa, que possibilitou a execução de código arbitrário na urna eletrônica, podendo ser utilizado, por exemplo, para alterar as informações que são exibidas ao eleitor.

- Outro ataque, apesar de não ter sucesso, levou a sugestões importantes, como a sinalização de que o teclado perdeu contato com a placa mãe o uso do sinal soro de votação especificamente para esse fim.

Por fim, os resultados do teste de 2021 podem ser verificados em https://www.justicaeleitoral.jus.br/tps/arquivos/2021/tps-2021-relatorio-tecnico-de-avaliacao-geral.pdf:

- Foi possível fazer com que o boletim de urna fosse gerado sem criptografia, um parâmetro de configuração que existia para eleições comunitárias.
- Foi criado um invólucro idêntico à parte frontal da urna eletrônica, que foi sobreposto ao teclado e registrou os votos do eleitor. Sem nenhum dispositivo de segurança (e sem visão do mesário), isso poderia ser instalado em uma seção.
- Foi possível capturar o certificado utilizado para se conectar à rede do TSE, mas o firewall não permitiu as conexões.
- Através do plug P2 da urna eletrônica, foi possível quebrar o sigilo do voto, revelando-o para todos os eleitores.

14. COMO TORNAR O PROCESSO MAIS TRANSPARENTE?

A discussão do voto impresso como forma de tornar o sistema mais transparente, quando desvinculada do caráter político e abordada do ponto de vista técnico, é uma discussão válida.

Uma primeira proposta envolve a impressão de um comprovante do voto em texto limpo, que o eleitor leva para casa. Essa proposta **não tem qualquer utilidade para auditar o resultado da eleição**, já que esse comprovante não pode ser recuperado depois para recontagem, **e também viola o sigilo do voto**. Por isso, ela jamais será implementada no mundo real.

Outra proposta envolve imprimir um comprovante de voto em texto limpo, que é auditado pelo eleitor antes de ser depositado em uma caixa de acrílico ou invalidado se o eleitor discordar do texto que o comprovante contém, podendo assim haver recontagem manual dos votos.

Essa proposta, sem outros mecanismos, é vulnerável, já que é possível, por exemplo, inserir cédulas inválidas na caixa de acrílico, além de que a contagem manual, por ser geralmente um processo impreciso, pode retornar resultados incongruentes e ser utilizada para deslegitimar o candidato vencedor.

Entretanto, é possível produzir uma proposta que garante todas essas características e evita fraudes não especializadas (como a inserção ou remoção de votos da urna). A seguir, demonstraremos como um sistema do tipo funciona, apresentando o passo a passo para que um eleitor vote.

Primeiramente, o eleitor se dirige à urna eletrônica com sua escolha. Ele insere os dados de sua escolha normalmente e, ao final do processo, a máquina imprime uma cédula composta de duas partes.

Na primeira parte, há o voto do eleitor v e uma série de metadados em texto simples seguido de um QR Code que resume esses dados, além de uma hash e uma assinatura digital feita a partir de uma chave privada da urna. Na segunda, há o mesmo voto escrito de forma cifrada e, também na forma de um QR Code. O valor do voto de forma cifrada assume a forma $e = E(v, r)$, em que E é uma criptografia de chave pública, e r é um valor aleatório gerado pela urna, de forma que dois votos iguais não produzem o mesmo valor e.

Figura 16: esse comprovante é impresso, e o eleitor pode observá-lo através do acrílico.

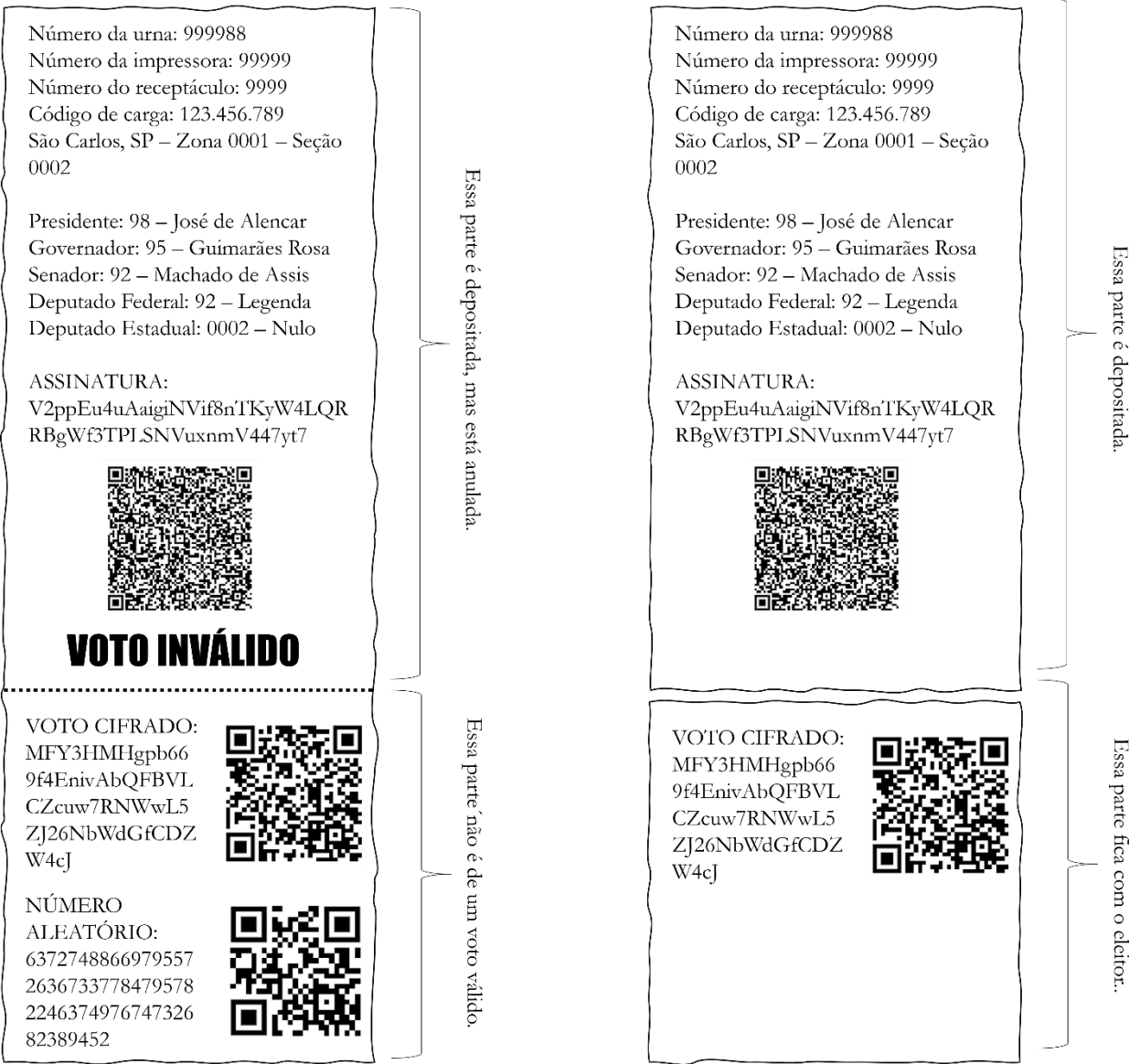
Número da urna: 999988
Número da impressora: 99999
Número do receptáculo: 9999
Código de carga: 123.456.789
São Carlos, SP – Zona 0001 – Seção 0002

Presidente: 98 – José de Alencar
Governador: 95 – Guimarães Rosa
Senador: 92 – Machado de Assis
Deputado Federal: 92 – Legenda
Deputado Estadual: 0002 – Nulo

ASSINATURA:
V2ppEu4uAaigiNVif8nTKyW4LQR
RBgWf3TPLSNVuxnmV447yt7

VOTO CIFRADO:
MFY3HMHgpb66
9f4EnivAbQFBVL
CZcuw7RNWwL5
ZJ26NbWdGfCDZ
W4cJ

O eleitor, então, tem duas escolhas: auditar seu voto, ou depositá-lo. Se o eleitor optar por auditar, a urna imprime o valor de r e anula a cédula impressa de forma que o eleitor pode, utilizando um aplicativo da própria seção ou próprio, conferir que a tupla (v, r) de fato é encriptada para e. Como isso quebra o sigilo daquele voto, a cédula precisa ser anulada antes de ser depositada na urna. Se o eleitor optar por depositar, a urna computa o voto cifrado eletronicamente, corta o voto impresso, deposita a parte superior em uma urna física e dá a parte inferior para o eleitor.

Figura 17: o que acontece se o eleitor audita (esquerda) ou deposita (direita) o voto.

Dessa forma, o eleitor sempre pode desafiar a urna a provar que o voto dele está sendo cifrado corretamente, isto é, passando por um algoritmo preservando as escolhas que ele fez. Como é impossível prever se o eleitor irá auditar ou depositar seu voto, o equipamento precisa computar todos os votos corretamente. Porém, o sigilo do voto é preservado porque o voto a ser depositado nunca passa pelo processo de auditoria.

Ao final da eleição, é publicada uma lista de votos cifrados, onde o eleitor pode checar se seu voto está ali sem risco de ter seu voto decodificado, já que ele foi codificado utilizando um número aleatório que já se perdeu. A criptografia utilizada para produção dos votos cifrados é homomórfica, o que significa que ela preserva a propriedade:

$$E(m_1) \cdot E(m_2) = E(m_1 + m_2)$$

Em outras palavras: o produto de duas ou mais mensagens cifradas é igual ao ciframento da soma dessas mensagens. Assim, a autoridade eleitoral apenas multiplica o valor dos votos cifrados, e decifra esse produto – para então chegar no total de votos que cada candidato teve.

Qualquer pessoa pode, assim, fazer o processo inverso: partir do total de votos e checar, utilizando a chave pública, que esse valor criptografado retorna o produto dos votos individuais.

Para tornar o processo ainda mais seguro, pode-se utilizar n chaves públicas de n agentes diferentes para fazer o ciframento dos votos, de forma que nenhum agente sozinho é capaz de decifrar o voto individual de um eleitor. É preciso que n agentes se corrompam para que seja possível decifrar cada voto individualmente, já que $n - 1$ agentes corruptos ainda não é suficiente.

Por fim, a presença de uma assinatura digital em cada voto impresso garante que aquele voto foi de fato produzido por uma urna, e torna difícil a possibilidade de inserir votos fraudados dentro do recipiente. Em uma eventual contagem de votos, um sistema de leitura automatizado é utilizado para eliminar erros humanos e fazer a checagem de cada cédula. A

maioria dos especialistas inclusive argumenta que não é necessário gastar com a auditoria de todos os votos, sendo suficiente sortear seções para serem auditadas.

Figura 18: o eleitor, então, localiza seu voto cifrado na lista de votos cifrados. É impossível decifrar o voto do eleitor, e o eleitor tem garantia que seus votos são corretamente cifrados.

VOTO CIFRADO:
MFY3HMHgpb66
9f4EnivAbQFBVL
CZcuw7RNWwL5
ZJ26NbWdGfCDZ
W4cJ

LvYPiR2wew4vgte8aKpLUkPvY8Gwd4H5gT5QyCw
9QXnbQEZQYp

yErT8Ym4p6nY9ziK5y97TDTA22KQAUFSdnF6fA
eKaWwU36gLHj

fAUS6QzKDikaUtcp4MzMpJMR9P24cxxwB4J8vMZ
WC2vjiQzxfw

yGZS9RwUm6LPwWQpZHufaDHMJWHaphVVaSk
3Ne4dA9PBZbTqUm

v3tbJ5L4r5QVpu2Kaag9kSKAtgH8JVj4HXhQpQR
WEmq7m4jDTS

MFY3HMHgpb669f4EnivAbQFBVLCZcuw7RNWw
L5ZJ26NbWdGfCDZW4cJ

YqWaG4eURzPdbQXStKXX7WEuWEySe2SrV6MA
VREUygatrBjUwh

zhNEVXq8M8J2k5U8D3ZEmEhptwRKSpeeg5TWz
k8A4ALVZKTdzP

j3C4XFygxc8qVFkqEUpVtgUBRybz3jvdQMQLnXN
LkFkpgAdPYi

nLwVXYVJ4u5QEVun6cpATevNT92P4RmUqx5UG
wgwcnLxvBXFxFg

Por fim, alguns sugerem que a tecnologia *blockchain* pode ser utilizada para aumentar a segurança das urnas eletrônicas. Porém, fazer isso sem violar o sigilo do voto implica em registrar uma informação na *blockchain* com garantia de que ela não é alterada posteriormente, mas nada garante que a informação registrada na *blockchain* está correta em primeiro lugar – para ter essa garantia, o sigilo do voto seria violado.

15. CONCLUSÕES

Assim, podemos concluir que, até o momento, **não há quaisquer evidências de que o sistema eleitoral foi maliciosamente projetado para (a) fraudar uma eleição ou (b) conter vulnerabilidades**, bem como **não há evidências de que (c) as vulnerabilidades descobertas foram exploradas em uma eleição**.

Para evitar que (a) e (b) aconteçam, atualmente contamos com a possibilidade de auditoria do código fonte por parte de diversas entidades fiscalizadoras, além de – pela primeira vez – o trabalho de duas universidades de renome que fiscalizaram o código fonte em computadores próprios. Apesar de seguirmos em uma tendência em direção à transparência, esse trabalho ainda tem limitações e, até que o código não se torne aberto (uma atitude defendida por vários especialistas), é importante que o TSE se atente às observações feitas por essas instituições para melhorar o processo de auditoria.

Para evitar que existam vulnerabilidades dos tipos (b) e (c), temos os Teses Públicos de Segurança, nos quais qualquer brasileiro pode apresentar um plano de ataque para tentar explorar eventuais vulnerabilidades na urna eletrônica que, se descobertas, são corrigidas antes da eleição. Além disso, há uma cadeia de operações que limita muito o impacto da exploração de uma vulnerabilidade por parte de um atacante externo a dezenas de seções (se adulterar os cartões flash) ou a uma seção (se atacar a urna propriamente), além de mecanismos que interrompem o processo de votação ou deixam evidente a incongruência caso ela ocorra.

Toda eleição é marcada por um pequeno número de erros humanos por parte de mesários que impede que alguns eleitores exerçam seu direito ao voto, mas que é insuficiente para alterar o resultado de uma eleição.

Apesar disso, o sistema eleitoral brasileiro pode ser modificado para se tornar mais transparente e aumentar a confiabilidade do eleitor. A discussão sobre quais medidas devem ser implementadas para caminhar em direção a um sistema mais transparente sem violar qualquer princípio de uma eleição justa não deve ser política, mas sim técnica. Nessa área, existem diversas modificações, em diversos níveis, que nos aproximam desse objetivo.

Por fim, ao passo que lutar para que as diversas etapas do processo eleitoral sejam mais seguras e transparentes é uma causa perfeitamente legítima, usar essas falhas como pretexto para exigir a anulação de uma eleição cujo resultado não lhe agrada (e que não trouxe evidências de fraude) é uma atitude desonesta – afinal, todos os candidatos sabiam (ou deveriam saber) da natureza do processo eleitoral antes de concorrerem.